A Spectrum of IV&V Modeling Techniques

Mats Heimdahl (Co-PI)

Jimin Gao (RA)

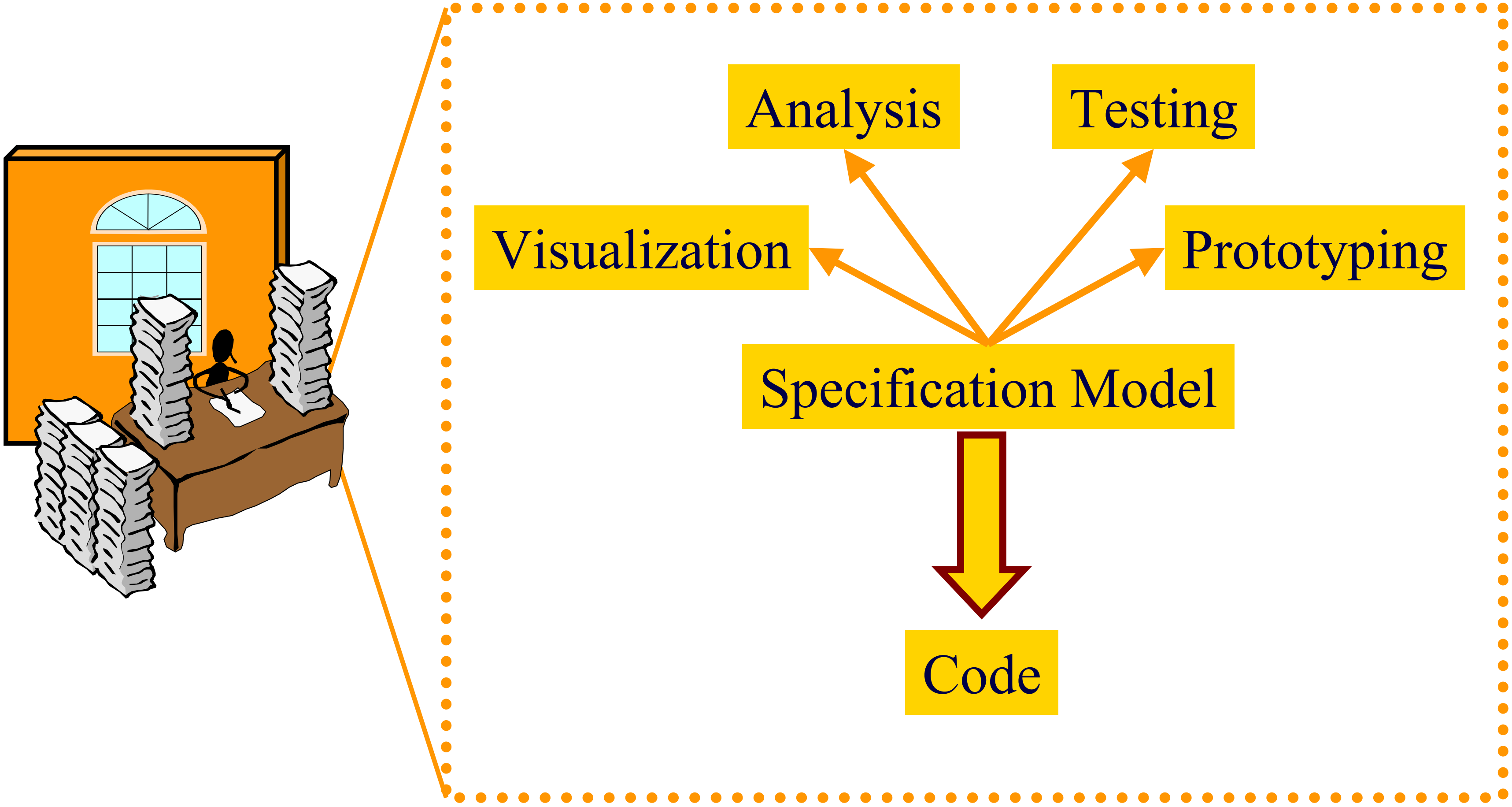
University of Minnesota

Tim Menzies (Co-PI)

David Owen (RA)

West Virginia University/NASA IV&V

Model-Based Development



Analysis

Testing

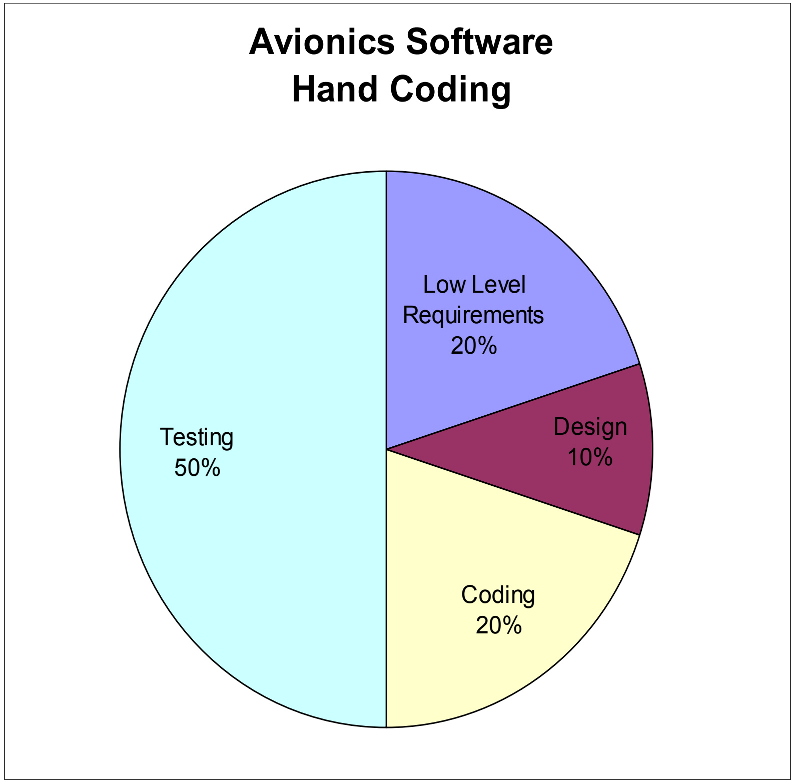
Visualization

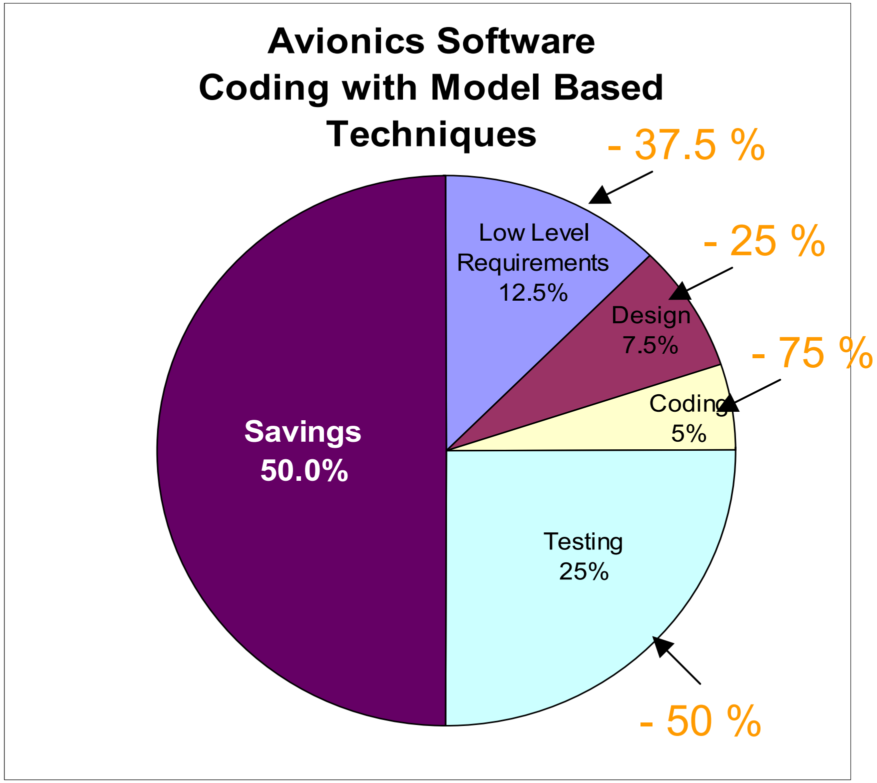
Prototyping

Specification Model

Code

ROI with Model Based Development





Source: Esterel Technologies

http://www.cs.umn.edu/crisys

Model-Based Development

Coming to projects everywhere—**soon**

- Model based development in some form will in the near future be the norm in critical systems development
  - Airbus Industries require the use of model based techniques from all vendors
  - Boeing currently evaluating **what** to require—not **if** they will require something
  - Honeywell and Rockwell Collins are fielding the capabilities within the next two years
  - Etc., etc.

Date: Fri, 2 May 2003 05:05:45 -0400
Subject:

JPL Welcomes World-Renowned Software Specialist

Jet Propulsion Laboratory, Pasadena, Calif.

Dr. Gerard Holzmann, a leader in software verification and validation, has joined NASA's Jet Propulsion Laboratory, Pasadena, Calif.

Holzmann will lead and conduct research, development and applications in software verification and validation.

The Association for Computing Machinery presented Holzmann with the prestigious Software Systems Award for development of Spin, a program devoted to the efficient detection of defects in network computers.

At 08:00 AM 5/5/2003 -0400, Nelson Keeler wrote:

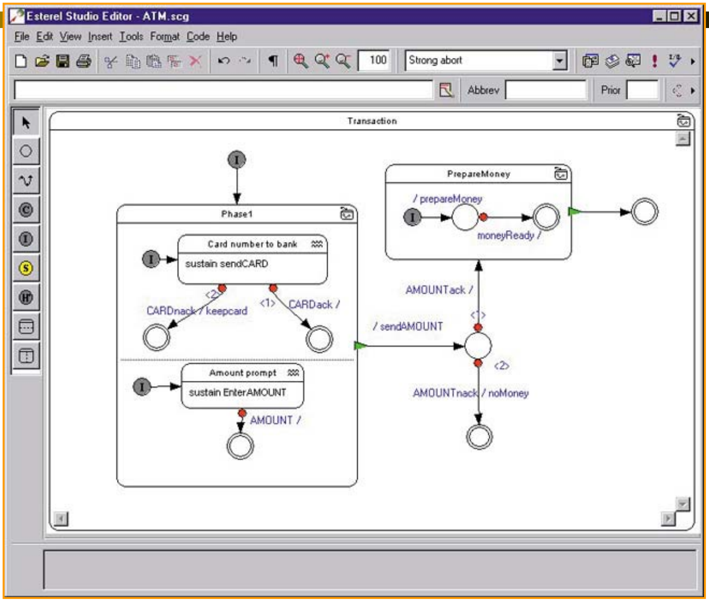
Will this make our work at JPL harder or easier?

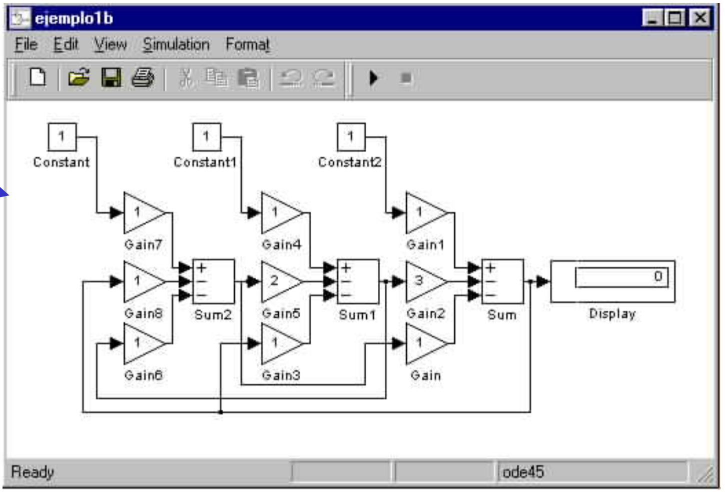
At 08:00 AM 5/5/2003 -0900, Timm writes:

harder- unless we can keep up with the boom in model-based methods

Model-Based Development Tools

- Commercial Products
  - Esterel Studio and SCADE Studio from Esterel Technologies
  - Rhapsody from I-Logix
  - Rose Real-Time from Rational
  - Simulink and Stateflow from Mathworks Inc.

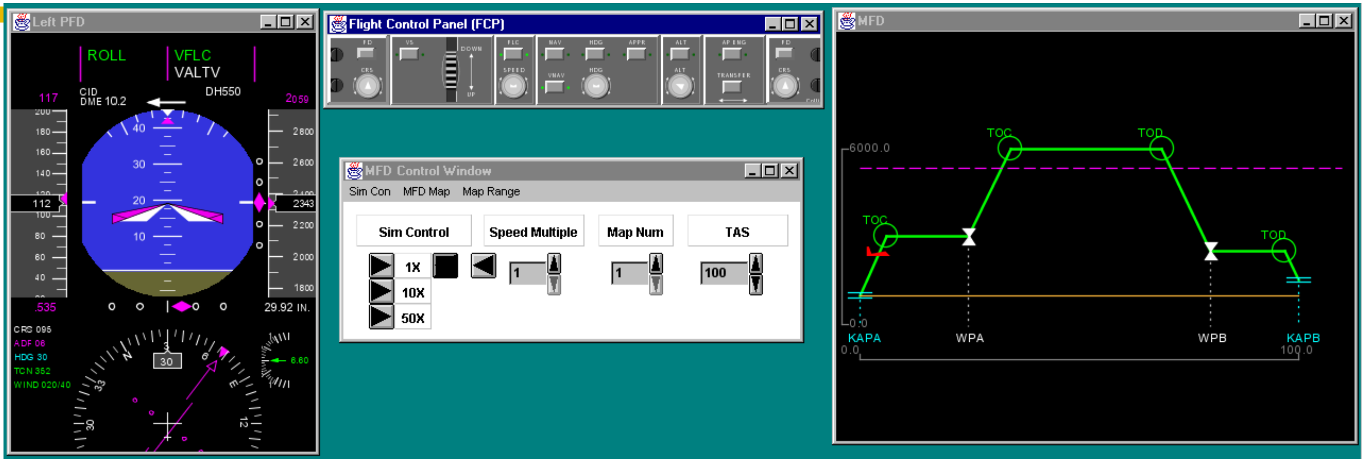




RSML^{-e} and Nimbus

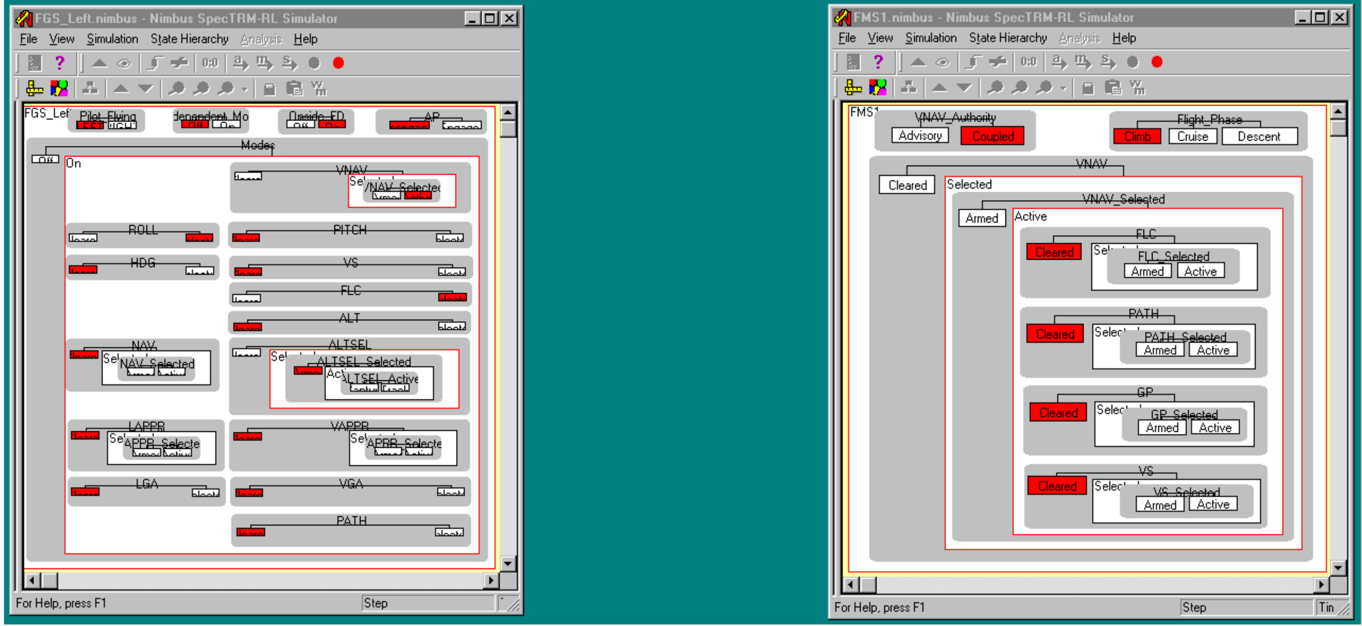
Project with Rockwell Collins Inc.

Java Simulations of environment



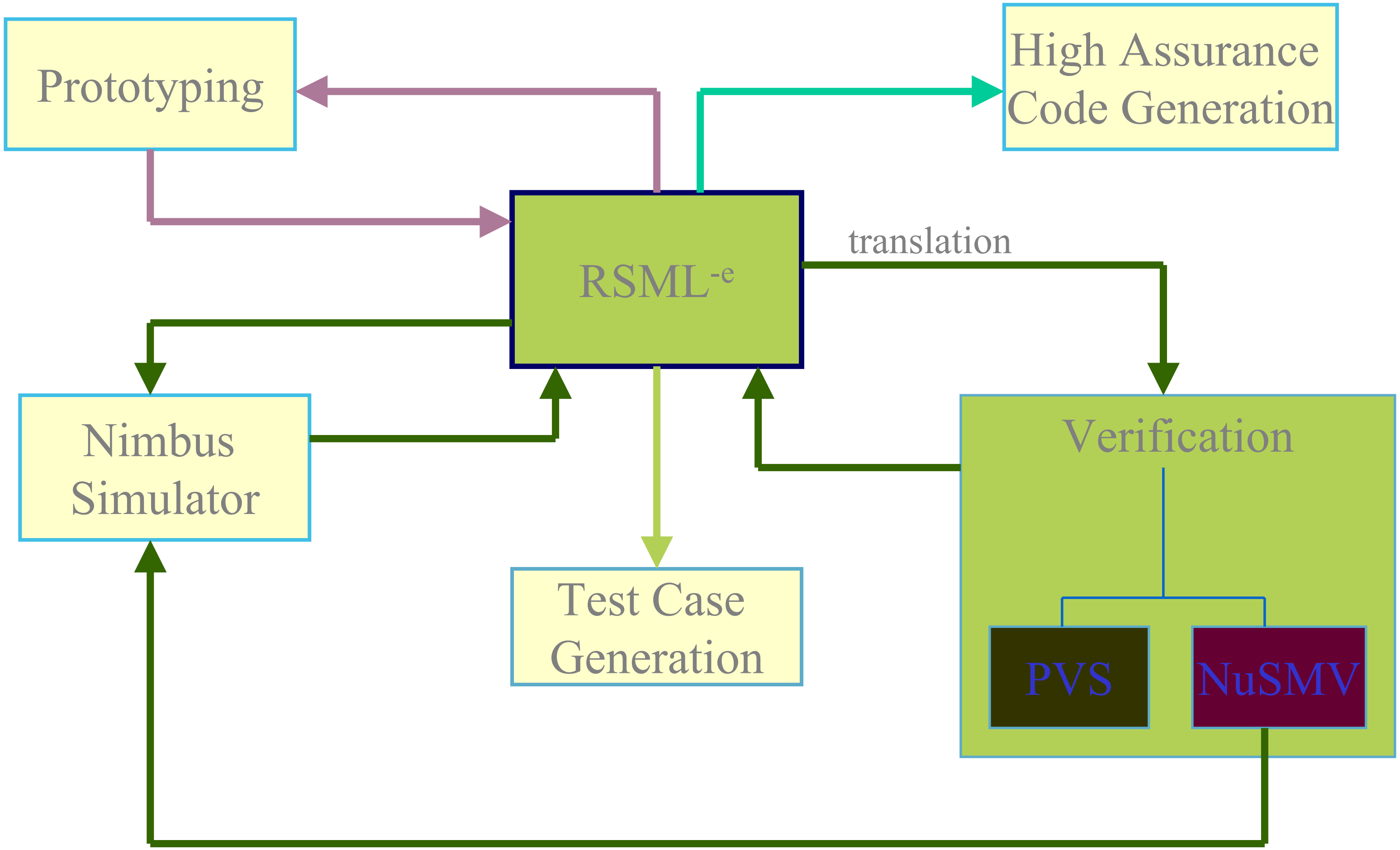
RSML^{-e} Formal Models (~20 running concurrently)

- Integration in MatLab
- Test case generation
- Model checking
- Theorem proving



http://www.cs.umn.edu/crisys

Specification Centered Software Development



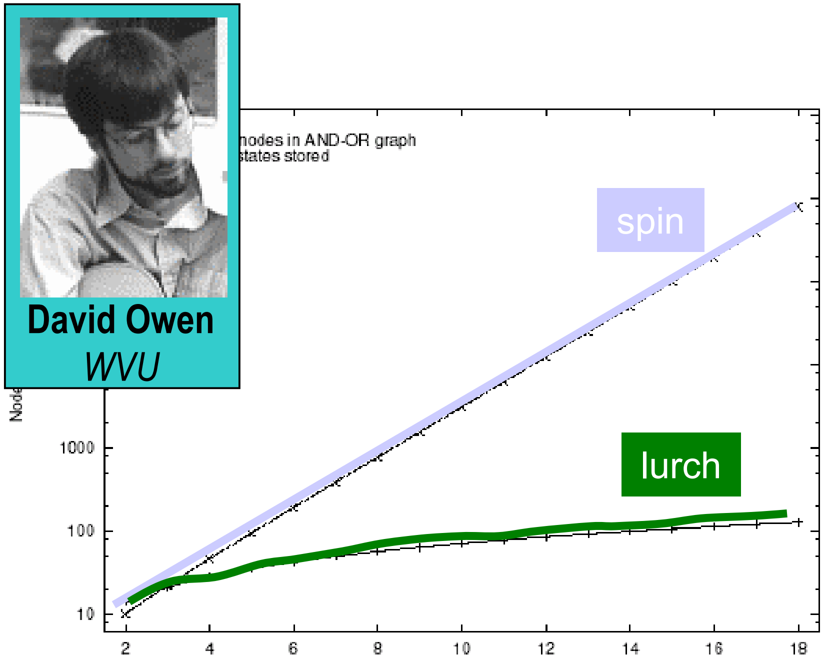
Formal Verification

- Model Checking
  - Exhaustive state space exploration
    - Tools—SMV, FormalCheck, SPIN, etc.
    - NASA Ames and JPL
  - State space explosion a problem
    - Verification effort exponential in problem size
- Theorem Proving
  - Guided tools for analytical proofs
    - Tools—PVS, ACL-2, HOL
    - NASA Langley
  - Generally quite difficult to use

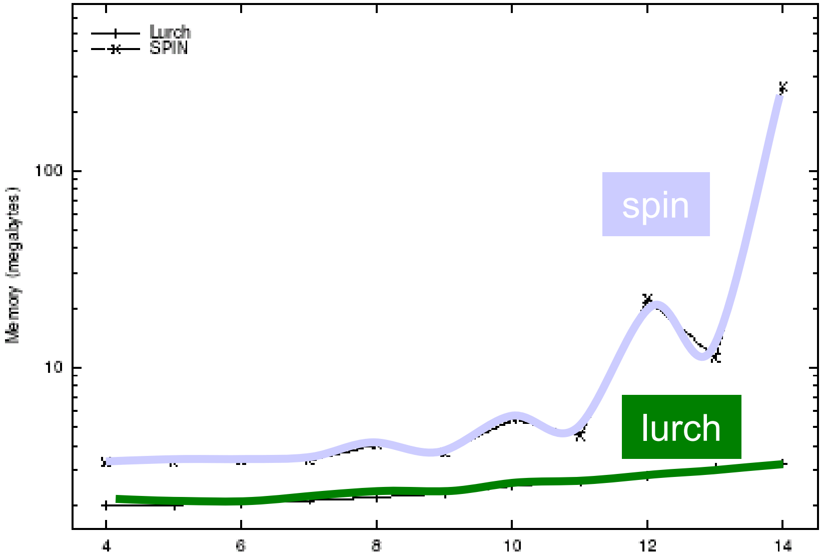
Alternative – LURCH

- Mathematical model of software
  - FSMs
- Internally, AND-OR graphs (compact)
- Repeat a few times
  - Reset
  - Run
  - Resolve conflicts at random

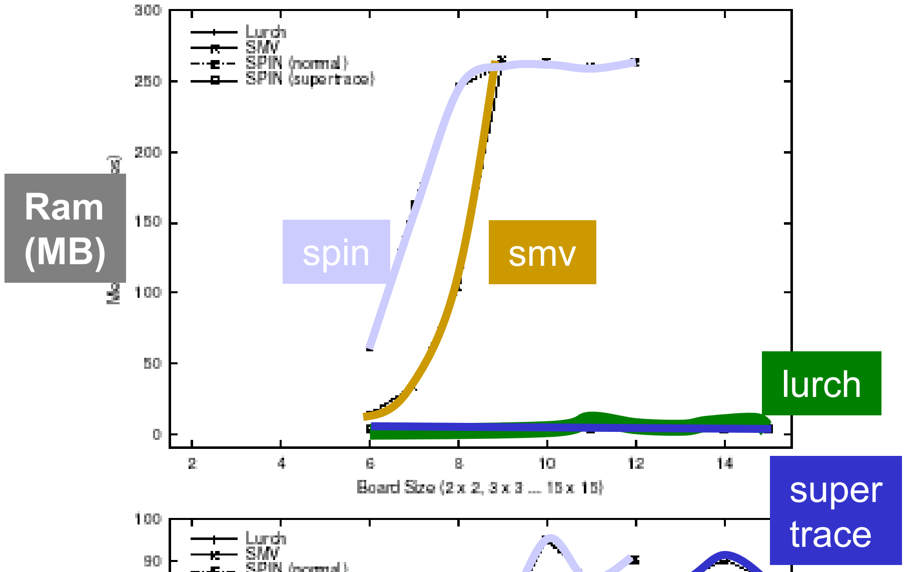
LURCH: son of HT0 (temporal properties)

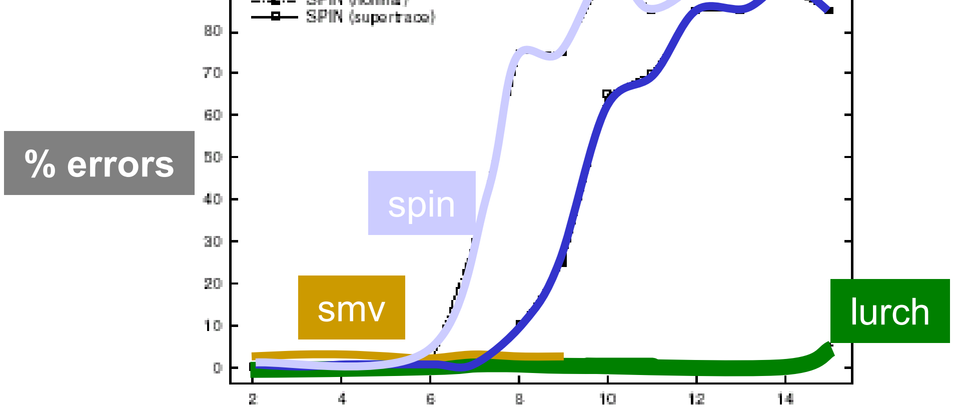


philosophers



nqueens n=: 4..14





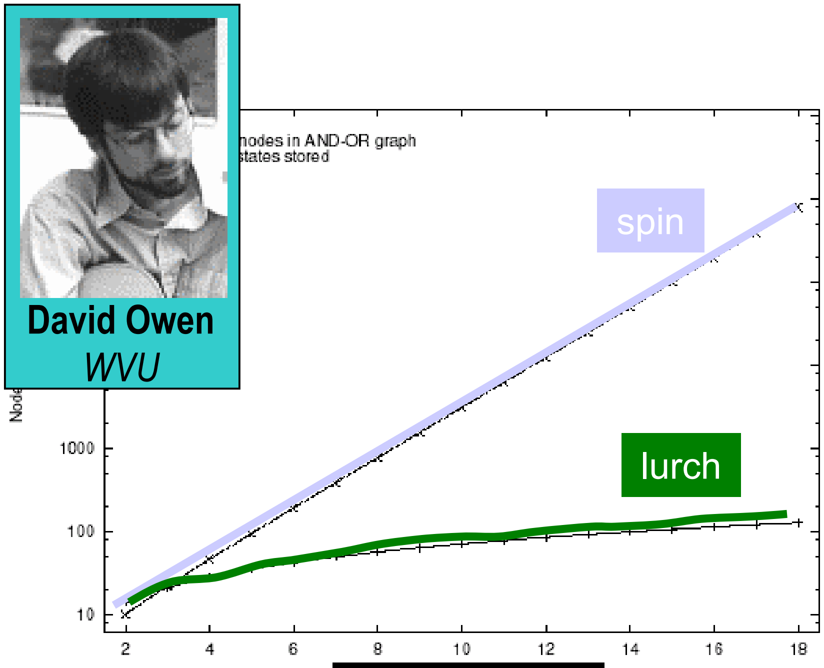
Tic-tac-toe board size: 2..15

The Question

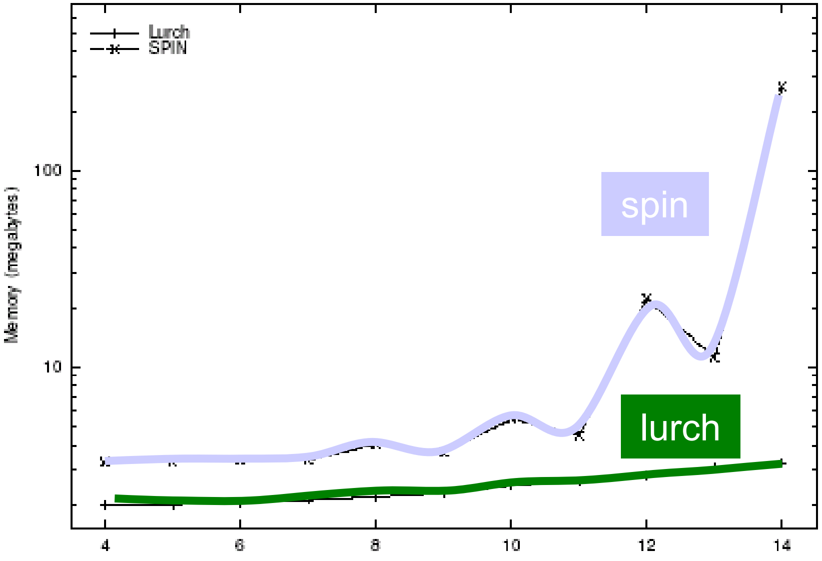
- Since Lurch is random—how many problems will it miss??

- Hypothesis:
- Problems are either very easy to find, or they are not likely to be not there at all
  - How likely?????

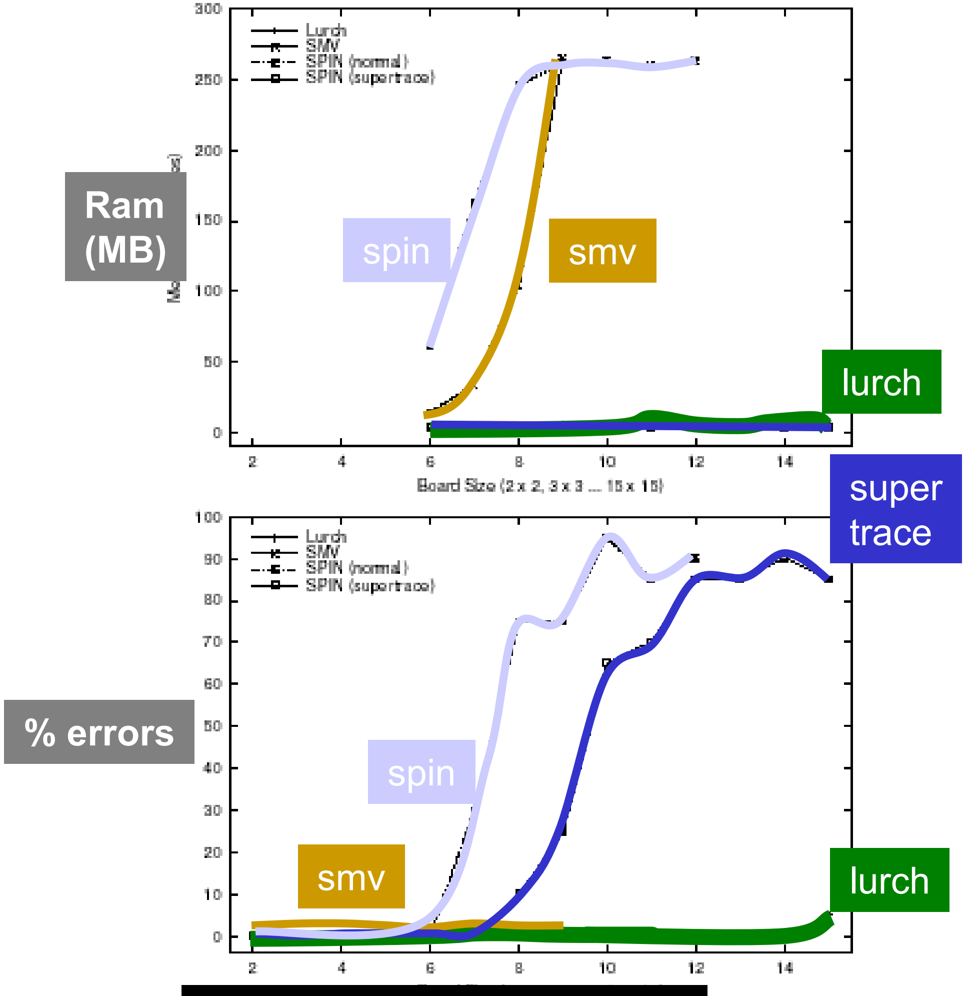
LURCH: son of HT0 (temporal properties)



philosophers



nqueens n=: 4..14



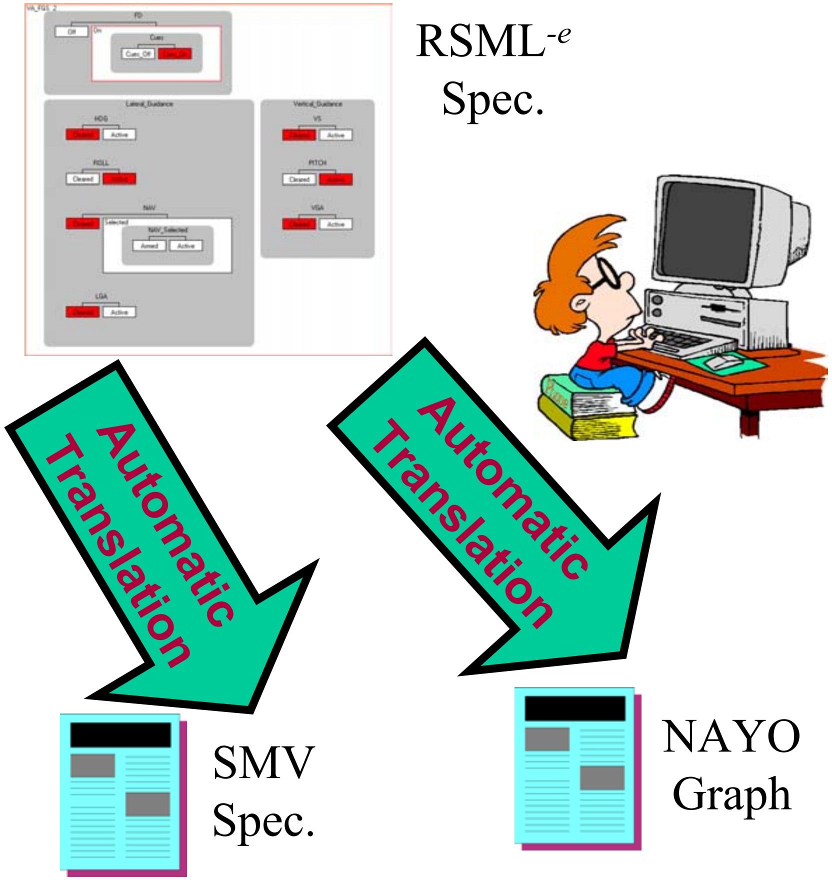
Tic-tac-toe board size: 2..15

Open Issue—Last Review

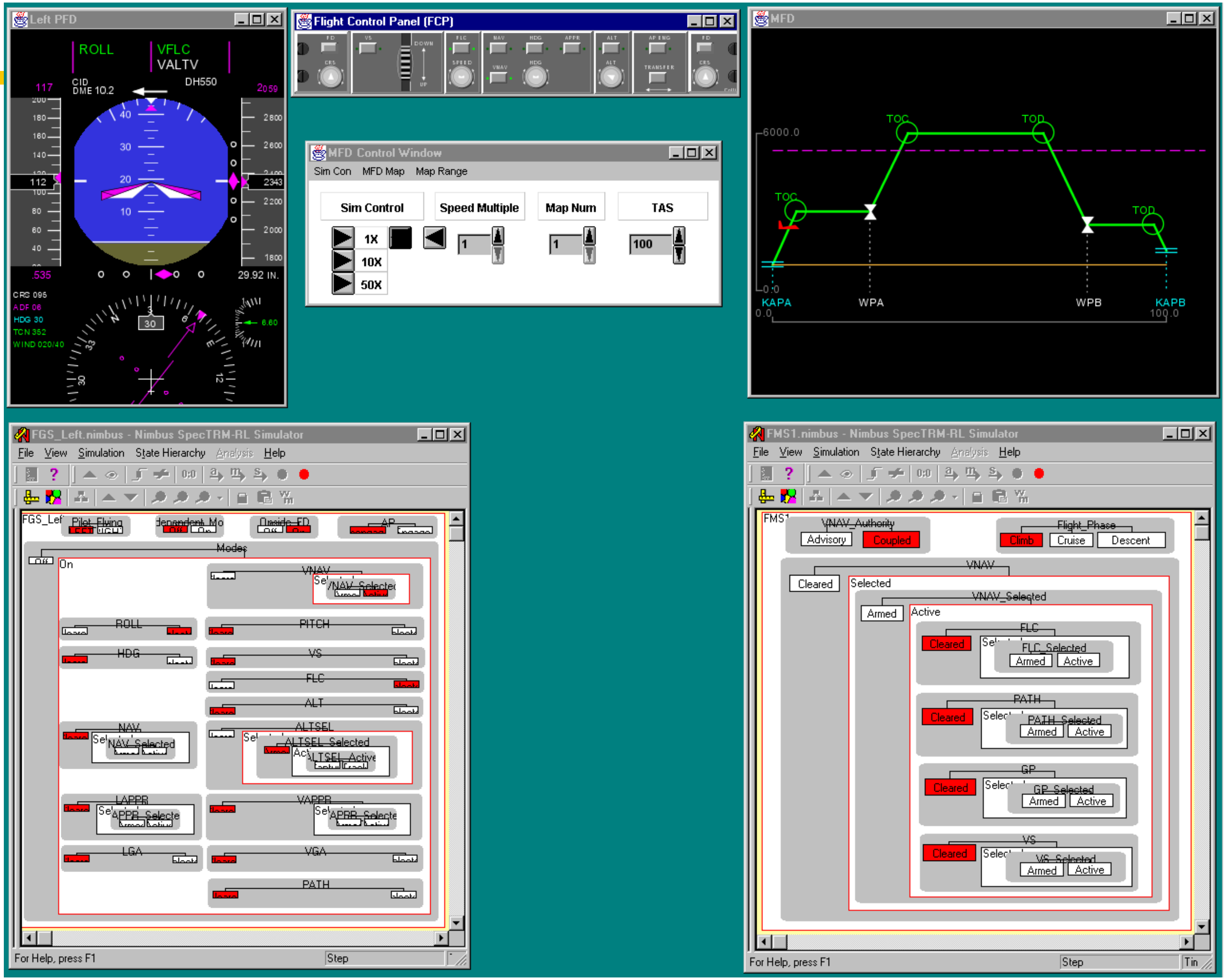
- If the random search does not find problems, are there none?
  - Compare the stochastic results with full verification on realistic models
  - Experiments using:
    - RSML^{-e}
    - Nimbus
    - SMV
    - Stochastic search
    - Flight guidance models from Rockwell Collins

Analysis Experiment

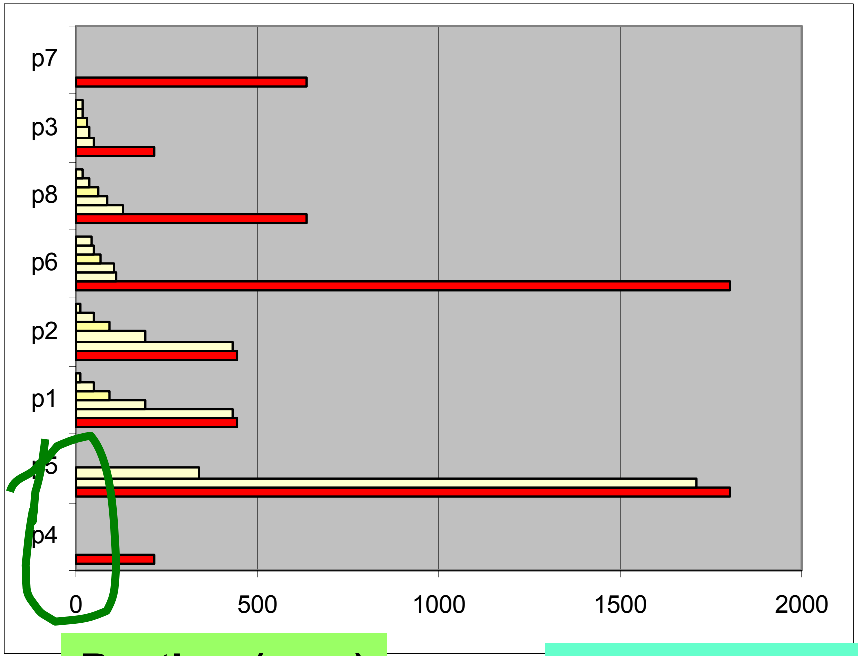
- **Available Resources:**
  - 6 RSML^{-e} models of Flight Guidance System from Rockwell Collins Inc.
  - Collection of desirable properties
  - Translator from RSML^{-e} to
    - SMV
    - FSM suitable for stochastic search
- **Experimental Method:**
  - Seed errors in the FGS models
  - Apply stochastic search as well as full formal verification
  - Compare performance and detection capability



Flight Guidance System



http://www.cs.umn.edu/crisys

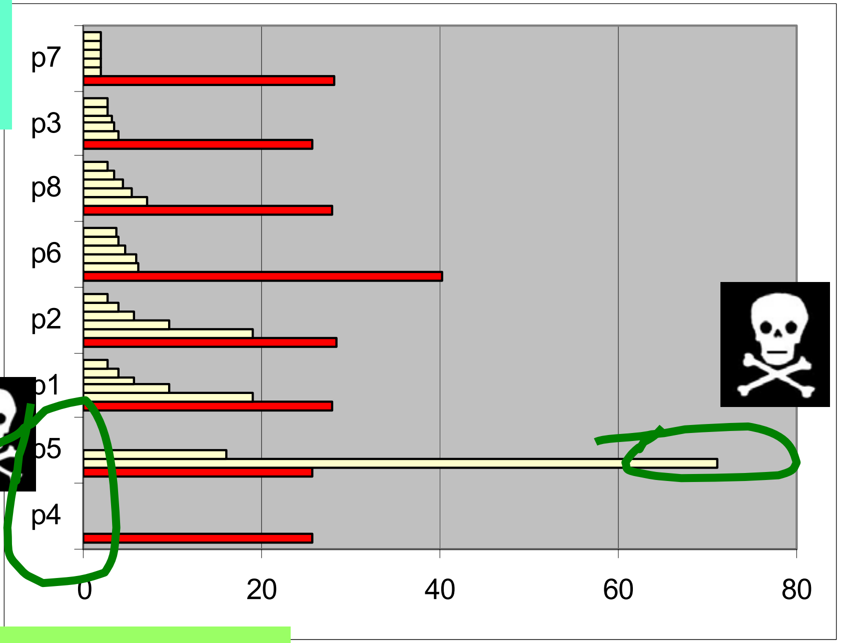


Runtime (secs)

NuSMV

Lurch (5 runs)

- **Sometimes, (8/40) random search failed**
- **Often, much faster**
- **Often, much smaller**



memory (MB)

Summary

- Hypothesis seems to hold
  - Most faults easy to find
- Huge impact for
  - Static analysis
    - Especially refutation
  - Stochastic testing
    - May be as effective as any other testing techniqu

- Stochastic state space exploration may hold the key
  - Initial experiments are very encouraging
- But, we need to explore further
  - Rigorous experiments are starting as I speak
- We may also evaluate alternative analysis tools
  - SAL from SRI